UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/608,459	06/27/2003	Brian D. Noble	UOM 0299 PUS	9384

22045 7590 10/17/2006

BROOKS KUSHMAN P.C.
1000 TOWN CENTER
TWENTY-SECOND FLOOR
SOUTHFIELD, MI 48075

EXAMINER	
GELAGAY, SHEWAYE	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 10/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/608,459	NOBLE ET AL.	
	Examiner	Art Unit	
	Shewaye Gelagay	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 June 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) *20-25* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3/22/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Election/Restrictions

1. Restriction to one of the following inventions is required under 35 U.S.C. 121:

   I. Claims 1-19, drawn to protecting application data stored on a portable computer, classified in class 713, subclass 193.

   II. Claims 20-25, drawn to an authorization token to prevent unauthorized access to resources of a system., classified in class 726, subclass 9.

2. The inventions are distinct, each from the other because of the following reasons:

Inventions Group 1 and Group 2 are related as combination and subcombination. Inventions in this relationship are distinct if it can be shown that (1) the combination as claimed does not require the particulars of the subcombination as claimed for patentability, and (2) that the subcombination has utility by itself or in other combinations (MPEP § 806.05(c)). In the instant case, the combination as claimed does not require the particulars of the subcombination as claimed because Group 1 is data protection wherein unauthorized access to information held in memory elements. Group 2 is used using tokens to prevent unauthorized access to resources of a system. The subcombination has separate utility such as Group 2 can be used to prevent unauthorized access to a network.

The examiner has required restriction between combination and subcombination inventions. Where applicant elects a subcombination, and claims thereto are subsequently found allowable, any claim(s) depending from or otherwise requiring all

the limitations of the allowable subcombination will be examined for patentability in accordance with 37 CFR 1.104. See MPEP § 821.04(a). Applicant is advised that if any claim presented in a continuation or divisional application is anticipated by, or includes all the limitations of, a claim that is allowable in the present application, such claim may be subject to provisional statutory and/or nonstatutory double patenting rejections over the claims of the instant application.

3. Because these inventions are independent or distinct for the reasons given above and there would be a serious burden on the examiner if restriction is not required because the inventions have acquired a separate status in the art in view of their different classification, restriction for examination purposes as indicated is proper.

4. During a telephone conversation with David R. Syrowik on 10/10/06 a provisional election was made without traverse to prosecute the invention of Group 1, claims 1-19. Affirmation of this election must be made by applicant in replying to this Office action. Claims 20-25 are withdrawn from further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

5. Applicant is reminded that upon the cancellation of claims to a non-elected invention, the inventorship must be amended in compliance with 37 CFR 1.48(b) if one or more of the currently named inventors is no longer an inventor of at least one claim remaining in the application. Any amendment of inventorship must be accompanied by a request under 37 CFR 1.48(b) and by the fee required under 37 CFR 1.17(i).

Double Patenting

6. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1-19 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-14 of copending application 10/119204. Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 1 and 12 of copending application 10/119204 and claims 1 and 12 of the instant application are functionally equivalent. The only difference in the two applications is that the instant application has in-memory portions of address space for an application program or data. Zadok teaches providing in-memory portions of address space for an application program. (section 2.1 Key Management) Therefore, it would have been obvious to one skilled in the art at the time the invention was made to modify the method disclosed by the copending application with Zadok in order to avoid

storing information related to encryption permanently thereby making the system more secure.

7. This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

The following table shows the complete mapping of the claims between the instant application and the copending application.

Instant Application 10/608459	Copending application (10/119204)
1. A system to maintain application data stored on a portable computer secure, the system comprising: an authorization client for use on the portable computer for making requests, the portable computer being capable of providing in-memory portions of address space for an application program; a security device to be associated with an authorized user of the portable computer and including an authorization server for supplying responses to the requests; a communication subsystem for wirelessly communicating the requests and the responses to the server and the client, respectively, within a range; and a cryptographic subsystem for encrypting data located in the in-memory portions of the address space to obtain corresponding encrypted data when the security device is outside the range of the communication subsystem and for decrypting the encrypted data when the security device is back within the range.	1. A system to maintain data stored on a portable computer secure, the system comprising: an authorization client for use on the portable computer for making requests; a security device to be associated with an authorized user of the portable computer and including an authorization server for supplying responses to the requests; a communication subsystem for wirelessly communicating the requests and the responses to the server and the client, respectively, within a range; and a cryptographic subsystem for use on the portable computer for encrypting the data to obtain corresponding encrypted data when the security device is outside the range of the communication subsystem and for decrypting the encrypted data when the security device is back within the range.
2. The system as claimed in claim 1 wherein the requests include cryptographic requests for cryptographic information and wherein the server supplies the cryptographic information in response to	2. The system as claimed in claim 1 wherein the requests include cryptographic requests for cryptographic information and wherein the server supplies the cryptographic information in response to

the cryptographic requests and wherein the cryptographic subsystem utilizes the cryptographic information to either encrypt or decrypt the data.	the cryptographic requests and wherein the cryptographic subsystem utilizes the cryptographic information to either encrypt or decrypt the data.
3. The system as claimed in claim 1 further comprising means for suspending substantially all authorized user processes on the computer when the security device is outside the range and means for restarting the suspended authorized user processes on the computer when the security device is back within the range.	3. The system as claimed in claim 1 wherein the requests include polling requests.
4. The system as claimed in claim 2 wherein the cryptographic information includes keys.	4. The system as claimed in claim 2 wherein the cryptographic information includes keys.
5. The system as claimed in claim 4 wherein the keys are encrypted.	5. The system as claimed in claim 4 wherein the keys are encrypted.
6. The system as claimed in claim 1 further comprising means for suspending selected authorized user processes on the computer when the security device is outside the range and means for restarting the selected authorized user processes on the computer when the security device is back within the range.	6. The system as claimed in claim 4 wherein the keys include user and group keys.
7. The system as claimed in claim 1 further comprising a mechanism for establishing a binding between the portable computer and the security device to ensure that the security device only responds to a portable computer with a valid binding.	7. The system as claimed in claim 1 further comprising a mechanism for establishing a binding between the portable computer and the security device to ensure that the security device only responds to a portable computer with a valid binding.
8. The system as claimed in claim 1 wherein the security device is an authorization token.	8. The system as claimed in claim 1 wherein the security device is an authorization token.
9. The system as claimed in claim 4 wherein the keys include at least one master key.	9. The system as claimed in claim 2 wherein the computer has a low speed memory and high speed memory and wherein the data stored in the high speed memory is not encrypted and the data stored in the low speed memory is encrypted.
10. The system as claimed in claim 9	10. The system as claimed in claim 2

wherein the at least one master key is a key-encrypting key.	wherein the cryptographic subsystem includes encrypted keys and wherein the cryptographic information includes keys for decrypting the encrypted keys.
11. The system as claimed in claim 2 wherein the cryptographic subsystem includes encrypted keys and wherein the cryptographic information includes keys for decrypting the encrypted keys.	11. The system as claimed in claim 1 wherein the requests including the polling requests are encrypted.
12. A method to maintain application data stored on a portable computer secure, the method comprising: providing an authorization client for use on the portable computer for making requests, the portable computer being capable of providing in-memory portions of address space for an application program; providing a security device to be associated with an authorized user of the portable computer and including an authorization server for supplying responses to the requests; wirelessly communicating the requests and the responses to the server and the client, respectively, within a range; encrypting data located in the in-memory portions of the address space to obtain corresponding encrypted data when the security device is outside the range; and decrypting the encrypted data when the security device is back within the range.	12. A method to maintain data stored on a portable computer secure, the method comprising: providing an authorization client for use on the portable computer for making requests; providing a security device to be associated with an authorized user of the portable computer and including an authorization server for supplying responses to the requests; wirelessly communicating the requests and the responses to the server and the client, respectively, within a range; encrypting the data to obtain corresponding encrypted data when the security device is outside the range; and decrypting the encrypted data when the security device is back within the range.
13. The method as claimed in claim 12 further comprising suspending substantially all authorized user processes on the computer when the security device is outside the range and restarting the suspended authorized user processes on the computer when the security device is back within the range.	13. The method as claimed in claim 12 wherein the requests include cryptographic requests for cryptographic information and wherein the server supplies the cryptographic information in response to the cryptographic requests and where-in the cryptographic information is used to either encrypt or decrypt the data.
14. The method as claimed in claim 12 wherein the requests include cryptographic requests for cryptographic information and wherein the server supplies the cryptographic information in response to	14. The method as claimed in claim 12 further comprising establishing a binding between the portable computer and the security device to ensure that the security device only responds to a portable

the cryptographic requests and wherein the cryptographic information is used to either encrypt or decrypt the data.	computer with a valid binding.
15. The method as claimed in claim 12 further comprising establishing a binding between the portable computer and the security device to ensure that the security device only responds to a portable computer with a valid binding.	
16. The method as claimed in claim 12 further comprising suspending selected authorized user processes on the computer when the security device is outside the range and restarting the selected authorized user processes on the computer when the security device is back within the range.	
17. The method as claimed in claim 14 wherein the cryptographic information includes keys.	
18. The method as claimed in claim 17 wherein the keys include at least one master key.	
19. The method as claimed in claim 18 wherein the at least one master key is a key-encrypting key.	

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1-6, 8, 11-14 and 16-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et al. (hereinafter Davis) U.S. Patent 6,088,450 in view of Zadok et al., Cryptfs: A Stackable Vnode (hereinafter Zadok) and in view of Teppler U.S. Patent 6,792,536.

As per claims 1 and 12:

Davis teaches a system to maintain application data stored on a portable computer secure, the system comprising:

an authorization client for use on the portable computer for making requests, the portable computer being capable of providing in-memory portions of address space for an application program; (figure 1, item 110; col. 2, lines 40-45)

a security device to be associated with an authorized user of the portable computer and including an authorization server for supplying responses to the requests; (figure 1, item 120; col. 3, lines 45-48)

a communication subsystem for wirelessly communicating the requests and the responses to the server and the client, respectively, within a range; (figure 1, item 140; col. 3, line 66-col. 4, line 2) and

a cryptographic subsystem for encrypting and decrypting data; (col. 3, lines 12-27; col. 4, lines 2-19)

Davis does not explicitly disclose providing in-memory portions of address space for an application program or data. Zadok teaches providing in-memory portions of address space for an application program. (section 2.1 Key Management) Therefore, it would have been obvious to one skilled in the art at the time the invention was made to

modify the method disclosed by Davis with Zadok in order to avoid storing information related to encryption permanently thereby making the system more secure (section 1. Introduction; Zadok)

Both references do not explicitly disclose encrypting data when the security device is outside the range of the communication subsystem and for decrypting the encrypted data when the security device is back with the range. Teppler in analogous art, however, discloses encrypting data when the security device is outside the range of the communication subsystem and for decrypting the encrypted data when the security device is back with the range. (col. 35, lines 25-47) Therefore, it would have been obvious to one skilled in the art at the time the invention was made to modify the method disclosed by Davis and Zadok with Teppler in order to mitigate the likelihood of unauthorized use of an electronic device by periodically checking for credential. (col. 1, lines 25-28; Davis)

As per claims 2 and 13-14:

The combination of Davis, Zadok and Teppler teaches all the subject matter as discussed above. In addition, Davis further discloses a system wherein the requests include cryptographic requests for cryptographic information and wherein the server supplies the cryptographic information in response to the cryptographic requests and wherein the cryptographic subsystem utilizes the cryptographic information to either encrypt or decrypt the data. (col. 6, line 51-col. 7, line 10)

As per claims 3, 6 and 16:

The combination of Davis, Zadok and Teppler teaches all the subject matter as discussed above. In addition, Davis further discloses a system comprising means for suspending substantially all authorized user processes on the computer when the security device is outside the range and means for restarting the suspended authorized user processes on the computer when the security device is back within the range. (col. 6, lines 33-34)

As per claims 4 and 17:

The combination of Davis, Zadok and Teppler teaches all the subject matter as discussed above. In addition, Davis further discloses a system wherein the cryptographic information includes keys. (col. 5, lines 34-49)

As per claims 5 and 11:

The combination of Davis, Zadok and Teppler teaches all the subject matter as discussed above. In addition, Davis further discloses a system wherein the keys are encrypted. (col. 3, lines 35-37)

As per claim 8:

The combination of Davis, Zadok and Teppler teaches all the subject matter as discussed above. In addition, Davis further discloses a system wherein the security device is an authorization token. (Abstract)

10. Claims 7 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et al. (hereinafter Davis) U.S. Patent 6,088,450 in view of Zadok et al., Cryptfs: A

Stackable Vnode (hereinafter Zadok) and in view of Teppler U.S. Patent 6,792,536 and further in view of Tagawa et al. (hereinafter Tagawa) U.S. Patent Number 7,096,504.

As per claims 7 and 15:

The combination of Davis, Zadok and Teppler teaches all the subject matter as discussed above. None of the references explicitly disclose a system comprising a mechanism for establishing a binding between the portable computer and the security device to ensure that the security device only responds to a portable computer with a valid binding. Tagawa in analogous art, however, discloses a system comprising a mechanism for establishing a binding between the portable computer and the security device to ensure that the security device only responds to a portable computer with a valid binding. (col. 7, lines 62-67) Therefore, it would have been obvious to one skilled in the art at the time the invention was made to modify the method disclosed by Davis, Zadok and Teppler with Tagawa in order to verify the authenticity of both devices and if either of the device is invalid to stop the process. (col. 7, line 66; Tagawa)

11. Claims 9-10 and 18-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et al. (hereinafter Davis) U.S. Patent 6,088,450 in view of Zadok et al., Cryptfs: A Stackable Vnode (hereinafter Zadok) and in view of Teppler U.S. Patent 6,792,536 and further in view of Masuda et al. (hereinafter Masuda) U.S. Patent Number 6,714,649.

As per claims 9 and 18:

The combination of Davis, Zadok and Teppler teaches all the subject matter as discussed above. None of the references explicitly disclose a system wherein the keys include at least one master key. Masuda in analogous art, however, discloses a system wherein the keys include at least one master key. (col. 2, lines 20-24) Therefore, it would have been obvious to one skilled in the art at the time the invention was made to modify the method disclosed by Davis, Zadok and Teppler with Masuda in order to provide a system for enhancing the security of stored data for subsequent use in the user device. (col. 2, lines 22-23; Masuda)

As per claims 10 and 19:

The combination of Davis, Zadok, Teppler and Masuda teaches all the subject matter as discussed above. wherein the at least one master key is a key-encrypting key. (col. 2, lines 20-24)

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See Form PTO-892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shewaye Gelagay

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER